APPENDIX 3 TO SCHEDULE 3.3
TO THE
COMPREHENSIVE INFRASTRUCTURE AGREEMENT

SECURITY SERVICES SOW

DETAILED PACKAGE DRAFT

Table of Contents

List of Tables

This is Appendix 3 (Security Services SOW) to Schedule 3.3 (Statements of Work) to the Comprehensive Infrastructure Agreement between the Commonwealth and Vendor (the "Agreement"). Unless otherwise expressly defined herein, the capitalized terms used herein shall have the meaning assigned to them in Appendix 10 (SOW Definitions) to Schedule 3.3 or in the Agreement.

1.0 Security Services Overview and Objectives

1.1 Services Overview

This Appendix 3 (Security Services SOW) is the Statement of Work (or "SOW") that sets forth the roles and responsibilities of the Parties for the security services ("Security Services") provided under the Agreement as part of the Services. Security Services are the operations, administration and governance services and activities, as further detailed in this SOW, required to provide and support security to the Commonwealth's IT infrastructure and enterprise. Vendor shall provide Security Services that include:

1. Incident Management
   - Incident Management
   - Intrusion Detection
   - Intrusion Prevention
   - Virus response and Alert
2. Secure Infrastructure
   - Security technology
   - Security architecture
   - Security configuration
   - Technical consultation
3. Security policies, standards, procedures, and access control
4. VITA Critical Infrastructure
   - Physical security (i.e., facilities access)
5. Security awareness & training
6. Risk Management
   - Risk Assessment
   - Vulnerability Assessment
   - Vulnerability Scanning

In addition to the services described in this SOW, the Vendor is responsible for providing the services described in Appendix 1 (Cross-Functional Services SOW) to Schedule 3.3.

1.2 Service Objectives

The following are the key high-level Service objectives Vendor shall ensure the Commonwealth achieves through the Security Services:

- Meet Commonwealth business and security requirements for reducing risk and maintaining compliance
- Reduce security incidents, improve security posture, data management and backup in the distributed environment
- Support business initiatives in accordance with applicable security standards

- Maintain the confidentiality, integrity and availability of Commonwealth Data

2.0 Service Environment

2.1 Scope of the Infrastructure to be Supported

This paragraph describes the scope of Services described in Section 2. This includes assets, facilities and locations, personnel, policies and procedures, licenses and agreements and work-in-process. Schedules and attachments are associated with each section to allow for quarterly updates and changes. The following sub-sections and related SOW Addenda further describe and scope the Security environment to be supported and/or with which Vendor shall comply. Service Environment Addenda are to be maintained by Vendor, reviewed with VITA, updated by Vendor and made available to VITA on a quarterly basis.

2.1.1 Hardware and Software

a. A listing and description of hardware used in the delivery of Security Services is provided in Addendum 1 – Hardware.

b. A listing and description of software and utilities used in the delivery of Security Services is provided in Addendum 2 – Software.

2.1.2 Service Locations and Environments

A description of Commonwealth facilities and the IT environments for which Vendor will provide Security Services is provided in Addendum 3 – Commonwealth Facilities and IT Environments.

2.1.3 Personnel

Vendor will be responsible for providing qualified, appropriately skilled staff with applicable certifications, clearances, and background checks as appropriate, to meet the roles and responsibilities and Service Levels set forth in this SOW.

2.1.4 Policies, Procedures and Standards

A description of the Commonwealth's current policies, procedures, standards and regulatory compliance requirements with which Security Services will comply is provided in Schedule 13 (Commonwealth Policies) to the Agreement and in the Procedures Manual.

2.1.5 Agreements and Licenses

A list of security related agreements and licenses is provided in Schedule 28.23 (Contracts) and Schedule 28.70 (Licenses).

2.1.6 Current Projects

Commonwealth currently has a number of security-related Current Projects planned or in progress that are included in the scope of this SOW and are the responsibility of

Vendor to complete within the time frames specified by Commonwealth. A list of these Current Projects is provided in Schedule 28.29 (Current Projects).

2.2 Baseline Information

The SOW Baseline data and the seven (7) year volume projections for all applicable Towers that the Vendor shall use for its pricing is located in Schedule 10.1B – Pricing Response Format Microsoft Excel workbook within the worksheet titled "7 Year Volume Projections."

3.0 Security Services

3.1 Service Descriptions and Roles & Responsibilities

Security Services include the following Services, activities and roles and responsibilities.

3.1.1 Security Services

The Security Services provided by Vendor under this SOW include the following:

a. Security Administration Services:
   - Security Advisories and Information Alert Services
   - Security Policy Enhancement Services

b. Policy Compliance and Enforcement Services:
   - Vulnerability / Risk Assessment Services
   - Validation and Status Services
   - Physical Security Controls
   - Logical Security Controls

c. Proactive / Active Security Services:
   - Event Logging
   - Intrusion Detection Services
   - Intrusion Detection Services (Network based)
   - Intrusion Detection Services (Host Based)
   - Intrusion Prevention Services
   - Vulnerability Scanning Services
   - Vulnerability and Penetration Testing Services
   - Vendor Alert Services

d. Security Response Services:
   - Security Incident Response Services
   - Vulnerability Remediation
   - Harmful / Malicious Code Response

e. IT Service Continuity and Disaster Recovery Services

3.1.2 General Responsibilities

The following table identifies General roles and responsibilities associated with this SOW. An "X" is placed in the column under the party that will be responsible for performing the task. Vendor responsibilities are indicated in the column labeled "Vendor".

Table 1. General Roles and Responsibilities

General Roles and Responsibilities	Vendor	VITA
Cross Functional Services		
1. Provide overall direction and oversight for the Commonwealth's Information Security program and for Vendor activities in support of this program		X
2. Conduct architectural reviews of all new and modified system and infrastructure designs prior to implementation, to ensure that such designs conform to the Commonwealth's Strategic Technology Architecture and that they meet the Commonwealth's business needs		X
3. Provide Services that support Commonwealth business needs, security, technical requirements, and End-User requirements	X	
4. Comply with VITA and Commonwealth policies and standards and regulations applicable to the Commonwealth for information, Systems, personnel, physical and technical security	X	
5. Conform to changes in laws, regulations and policies. Major changes shall be proposed on a project-by-project effort basis to alter the environment to conform to the new requirements.	X	
6. Report performance against Security Service Levels	X	
7. Participate in coordination of all changes to the IT infrastructure that may affect the Service Levels of any other Service area.	X	
8. Provide timely creation, updating, maintenance and provision of all appropriate project plans, project time and cost estimates, technical specifications, management documentation and management reporting in a form/format that is acceptable to VITA for all projects and major Service activities	X	
9. Coordinate Service delivery with Help Desks, as well as other support groups within each of the other Towers in coordination with Eligible Customers, VITA, and all appropriate third-parties, as necessary	X	
10. Provide VIP Support Services as necessary	X	
Data Network Services		
11. Recommend WAN/LAN/VPN/firewall, IDS/IPS/routers and switch requirements based on industry best practices and as requested	X	
12. Review and approve requirements for WAN/LAN/VPN/firewall, IDS/IPS/routers and switch services		X
Voice and Video Telecom Services		
13. Provide fraud prevention, detection and reporting	X	

3.1.3 IT Life Cycle Services - Security

3.1.3.1 Security Planning & Analysis

Security Planning and Analysis Services are the activities associated with research of new technical trends, products and services, such as hardware components, System Software, and Networks that offer opportunities to improve the efficiency and effectiveness of the Security Services. Security Planning and Analysis Services can also help support competitive business advantage and mitigate risks by reducing defects and improving the quality of security.

The following table identifies the roles and responsibilities that Vendor and VITA will perform.

Table 2. Security Planning and Analysis Roles and Responsibilities

Security Planning and Analysis Roles and Responsibilities	Vendor	VITA
1. Define Commonwealth requirements at the enterprise level for all Security Services (e.g., business, technology strategy, functional, availability, capacity, performance, backup and IT Continuity Service)		X
2. Provide infrastructure security planning and analysis installation and upgrade recommendations	X	
3. Review and approve infrastructure security planning and analysis installation and upgrade recommendations		X
4. Continuously monitor security trends through independent research; document and report on products and services with potential use for the Commonwealth as it aligns with the Commonwealth's business and technology strategy	X	
5. Perform feasibility studies for the implementation of new security technologies that best meet Commonwealth business needs and meet cost, performance and quality objectives	X	
6. Conduct technical and business planning sessions to establish security standards, architecture and project initiatives per the planning and analysis policies and procedures		X
7. Participate in technical and business planning sessions to establish security standards, architecture and project initiatives	X	
8. Conduct technical reviews and provide recommendations for improvements to the infrastructure that increase efficiency and effectiveness of security and reduce costs in accordance with planning and analysis policies and procedures	X	
9. Develop and maintain application security policies, planning, guidelines, and architecture		X
10. Recommend potential improvements to application security architecture	X	
11. Perform application security review to ensure compliance with Vendor-supported infrastructure requirements	X	

3.1.3.2 Requirements Definition

Requirements Definition Services are the activities associated with the assessment and definition of security requirements that also comply with regulatory, VITA and

Commonwealth policies. These requirements drive the technical design for the environment. The following table identifies Requirements Definition roles and responsibilities that Vendor and VITA will perform.

Table 3. Requirements Definition Roles and Responsibilities

Requirements Definition Roles and Responsibilities	Vendor	VITA
1. Ensure requirements meet VITA and Commonwealth security policies and standards	X	

3.1.3.3 Design Specifications

Design Specification Services are the activities and Deliverables associated with translating End-User and information System requirements into detailed technical specifications. The following table identifies Design Specifications roles and responsibilities that Vendor and VITA will perform.

Table 4. Design Specifications Roles and Responsibilities

Design Specification Roles and Responsibilities	Vendor	VITA
1. Develop and document technical design plans and environment configuration based on VITA and Commonwealth security requirements	X	

3.1.3.4 Integration and Testing

Integration and Testing Services are the activities associated with ensuring that all individual Commonwealth infrastructure components configured with or added to the infrastructure work together cohesively to achieve the intended results. The following table identifies Integration and Testing roles and responsibilities that Vendor and VITA will perform.

Table 5. Integration and Testing Roles and Responsibilities

Integration and Testing Roles and Responsibilities	Vendor	VITA
1. Conduct security testing for all new and upgraded equipment, Networks, Software and Services to include unit, System, integration and regression testing	X	
2. Evaluate all new and upgraded service components and services for compliance with VITA and Commonwealth security policies, regulations and procedures	X	
3. Approve all infrastructure changes as a result of integration testing and regression requirements		X
4. Adjust VITA and Commonwealth security policies, regulations and procedures to incorporate new service features and components.		X

3.1.3.5 Operations and Administration

Operations and Administration Services are the activities associated with providing a stable IT infrastructure and to effectively and efficiently perform procedures to ensure the Services meet Service Level targets and requirements. The following table identifies Operations and Administration roles and responsibilities that Vendor and VITA will perform.

Table 6. Operations and Administration Roles and Responsibilities

Operations and Administration Roles and Responsibilities	Vendor	VITA

Operations and Administration Roles and Responsibilities	Vendor	VITA
Cross Functional Services		
1. Recommend enterprise Service component management tools in such a fashion that security Incidents, Problems, issues and events are proactively identified, reported and resolved according to prescribed Service Levels	X	
2. Review and approve enterprise Service component management tools		X
3. Install and configure approved enterprise Service component management tools	X	
4. Audit Operations and Administration Polices for compliance with VITA and Commonwealth security policies and standards		X
5. Maintain and provide audit information including access, general logs, application logs in accordance with VITA and Commonwealth's security policies and standards	X	
6. Maintain and provide VITA with a copy of or access to any Vendor-supplied security documentation (including updates thereto)	X	
7. Provide disposition and sanitization of assets and related configuration documentation in accordance with VITA and Commonwealth's policies and standards	X	
Mainframe & Server Services		
8. Develop and document security monitoring procedures that meet requirements and adhere to defined security policies and standards	X	
9. Review and approve security monitoring procedures		X
10. Recommend and provide preventative measures for proactive monitoring and self-healing capabilities to limit outages due to security Incidents	X	
11. Approve recommended preventative and self-healing measures		X
12. Manage security of data both in transit or at rest	X	
13. Provide secure offsite storage for designated media and transport of media to offsite location, and secure media disposition, as required	X	
14. Set up and manage End-User accounts, perform access control, monitor files and disk space and manage transaction definitions	X	
Desktop Computing Services		
15. Perform LAN/Domain/OS administration support activities (e.g., IP addressing, file and print sharing, logon End-User-id and password maintenance) for all managed servers (e.g., file/print, email)	X	
16. Manage End-User accounts, disk space quotas and access control (OS, database, Middleware, file systems, disk space, etc.)	X	
Data Network Services		
17. Manage all Network devices in accordance with VITA's security oversight policies and standards	X	
18. Maintain IP addressing schemes, router configurations, routing tables, VPN configurations, etc.	X	
19. Manage End-User accounts as needed for access and maintaining Network resources (e.g., logon End-User-id and password maintenance)	X	

Operations and Administration Roles and Responsibilities	Vendor	VITA
20. Maintain and provide audit information including access, general logs, application logs in accordance with VITA and Commonwealth's security policies and standards	X	
Voice and Video Telecom Services		
21. Provide proactive and reactive Voice and VideoTelecom Services fraud and security management and reporting	X	
22. Manage End-User accounts (e.g., account set up, password resets, account deletions and terminations) and provide administrative support (online directory Services to maintain and update the directory in accordance Service Levels) for all Services contained in this SOW according to VITA and Commonwealth's security policies and standards	X	
23. Provide VITA with a detailed explanation of outages due to security Incidents that identify the regional impact, source of breach, and preventative measures being taken to prevent future similar Incidents and outages	X	
Help Desk Services		
24. Coordinate End-User account administration, activation, changes and terminations, including: password/account setup and reset, remote access connectivity, e-mail accounts, End-User IDs, password resets, remote paging devices, voicemail administration, telephone lines, SecurID cards, catalog quotations, etc.	X	
25. Create, change and delete End-User accounts per requests in accordance with VITA and Commonwealth's security policies and standards	X	
26. Reset passwords as required in accordance with VITA and Commonwealth's security policies and standards	X	

3.1.3.6 Environment and Facilities Support

Environment and Facilities Support Services are the activities associated with maintaining environmental requirements in connection with Security Services at the Commonwealth facilities. The following table identifies environment and facilities support roles and responsibilities that Vendor and the VITA will perform.

Table 7. Environmental and Facilities Support Roles and Responsibilities

Environmental and Facilities Support Roles and Responsibilities	Vendor	VITA
1. Develop and recommend environment and facilities improvement plans for Vendor-monitored Commonwealth facilities as needed to maintain an effective and secure computing environment	X	
2. Develop, recommend, and implement environment and facilities security plans and procedures for Vendor owned and/or managed facilities as needed to maintain an effective and secure computing environment in accordance with VITA and Commonwealth security policies and standards	X	
3. Review and approve Vendor environment and facilities security plans and recommended VITA and Commonwealth security improvement plans		X

3.1.3.7 Maintenance

Maintenance Services are the activities associated with the maintenance and repair of hardware, Software and Networks with respect to the Services. The following table identifies Maintenance roles and responsibilities that Vendor and VITA will perform.

Table 8. Maintenance Roles and Responsibilities

Maintenance Roles and Responsibilities	Vendor	VITA
1. Perform diagnostics and maintenance for all hardware, Software, peripherals, Networks and special purpose devices for Services as appropriate to security	X	
2. Perform product patch, "bug fix," service pack installation and upgrades to the current installed version	X	
3. Approve production rollout of patch, "bug fix", service pack installation and upgrades to the current installed version		X

3.1.4 Security Service Delivery (physical/logical access to security service components)

Security Delivery Services are the activities associated with physical and logical security of all Service components (hardware and Software) and data, virus protection, access protection and other Security Services in compliance with VITA and Commonwealth security requirements and all applicable regulatory requirements. The following table identifies security roles and responsibilities that Vendor and VITA will perform.

Table 9. Security Roles and Responsibilities

Security Roles and Responsibilities	Vendor	VITA
1. Define security requirements, standards, procedures and policies including regulatory requirements		X
2. Actively participate in industry standard security forums and End-User groups to remain up to date with current security trends, threats, common exploits and security policies and procedures	X	
3. Assist in developing security standards, policies, and procedures including industry best practices	X	
4. Provide a full-time security assessment group to conduct continual assessments of Eligible Customers' security effectiveness	X	
5. Provide a security customer service group dedicated to the Commonwealth's enterprise that will be the direct liaison with VITA's Security Services Directorate for Eligible Customers' security requirements	X	
6. Provide a direct liaison with Eligible Customers for security requirements		X
7. Conduct risk assessment to identify control or security gaps		X
8. Provide security plan and IT infrastructure based on VITA-specified security requirements, architecture, standards, procedures, policies, and Commonwealth, federal, State, and local requirements and risks	X	
9. Review and approve security plans and IT infrastructure		X

Security Roles and Responsibilities	Vendor	VITA
10. Implement physical and logical security plans consistent with VITA and Commonwealth security policies and industry standards (e.g. ISO 17799 and 15408)	X	
11. Establish access profiles and policies for adding, changing, enabling/disabling and deleting log-on access of End-Users		X
12. Perform log-on/security-level access changes as detailed in profiles and policies for all Services	X	
13. Provide and support VITA-approved COTS or Open Source security analysis, monitoring, and defense (NIDS/NIPS, HIDS/HIPS, firewalls, etc.) products introduced into the Commonwealth's System and Network infrastructure via the Change Management process	X	
14. Recommend new best practice security technology and products when available or as requested	X	
15. Log and report security violations to VITA per VITA and Commonwealth policies and standards	X	
16. Implement immediate measures to react to an identified security Incident and take actions to isolate and minimize the negative impact to the Commonwealth infrastructure in accordance with VITA security procedures	X	
17. Resolve violations of security and security policy which are determined to be internal to the Vendor	X	
18. Resolve violations of security and security policy which are determined to be internal to the Commonwealth		X
19. Escalate and resolve security violations that originate outside of the hosted Network(s) (e.g., denial of service attacks, spoofing, Web exploits) in accordance with VITA security procedures	X	
20. Review all security patches relevant to the Commonwealth IT environment and classify the need and speed in which the security patches should be installed as defined by security policies, standards, and best practices	X	
21. Install security patches in accordance with Commonwealth and VITA security requirements, standards, procedures and policies	X	
22. Perform periodic security audits		X
23. Maintain all documentation required for security audits and internal control and control testing	X	
24. Place and support systems with particularly sensitive data in controlled access areas. Only End-Users with current, authorized access permission will be allowed to enter these areas	X	
25. Allow third party security audits as authorized by the VITA Security Services Directorate	X	
26. Implement a "Security Awareness Program" that addresses the support and delivery within the Vendor's organization	X	
27. Contribute, as requested, to VITA in managing VITA's "Security Awareness Program" for the Commonwealth	X	

3.1.5 Network Security Services

3.1.5.1 Firewall Management

Firewall Management Services include firewall engineering and management and access control list engineering and management in compliance with VITA and Commonwealth policies and standards. The following table identifies the Firewall Management roles and responsibilities that Vendor and VITA will perform.

Table 10. Firewall Management Services Roles and Responsibilities

Firewall Management Services Roles and Responsibilities	Vendor	VITA
1. Recommend best practice firewall policies	X	
2. Develop Commonwealth-specific firewall polices and requirements		X
3. Approve firewall polices and standards		X
4. Provide Services in conformance to firewall policies and requirements	X	
5. Perform firewall engineering and firewall security design	X	
6. Assess firewall security and propose alternative security designs	X	
7. Review and approve firewall security designs		X
8. Review and approve firewall Access Control Lists (ACL) policies and rules sets for Vendor domain firewalls		X
9. Develop recommendations for improved security	X	
10. Review and approve recommendations for improved security		X
11. Establish and provide baselines and device-specific ACLs and rule sets for Commonwealth domain firewalls		X
12. Implement and maintain baselines and device-specific ACLs and rule sets in accordance with VITA and Commonwealth policies	X	
13. Review and approve any changes to the ACLs and rule sets		X

3.1.5.2 Security Intrusion Prevention Services

Security Intrusion Prevention Services include Network-based Intrusion Detection Service (NIDS), Host-based Intrusion Detection Service (HIDS), and Network / Host-based Intrusion Prevention Services (HIDS/HIPS). The following table identifies the Security Intrusion Prevention roles and responsibilities that Vendor and VITA will perform.

Table 11. Security Intrusion Prevention Services Roles and Responsibilities

Security Intrusion Prevention Services Roles and Responsibilities	Vendor	VITA
1. Develop policies and standards for Intrusion Detection / Prevention Services (IDS / IPS)	X	
2. Develop Commonwealth-specific Intrusion Detection and Prevention Services polices and requirements		X
3. Approve policies and standards for Intrusion Detection / Prevention Services		X
4. Provide Intrusion Detection / Prevention Services and reporting	X	
5. Allow for independent Intrusion Detection / Prevention Services	X	

Security Intrusion Prevention Services Roles and Responsibilities	Vendor	VITA
6. Develop recommendations for improved security methods as determined by IDS / IPS findings	X	
7. Review and approve recommendations for improved security methods		X
8. Implement approved recommendations	X	

3.1.5.3 Security Vulnerability & Penetration Services

Security Vulnerability & Penetration Services are the activities associated with testing the susceptibility of the Commonwealth's Systems and Networks to a specific attack or suite of attacks targeting all Commonwealth Internet address space as well as all Commonwealth Intranet address space using automated and custom methods. The following table identifies the Security Vulnerability and Penetration roles and responsibilities that Vendor and VITA will perform.

Table 12. Security Vulnerability & Penetration Services Roles and Responsibilities

Security Vulnerability & Penetration Services Roles and Responsibilities	Vendor	VITA
1. Develop policies for Security Vulnerability & Penetration testing	X	
2. Approve policies for Security Vulnerability & Penetration testing		X
3. Conduct security vulnerability scans & penetration testing using third party providers as necessary to demonstrate objectivity and validate results	X	
4. Conduct vulnerability & penetration testing as necessary to maintain current security posture	X	
5. Provide detailed reporting on Vulnerability Test & Penetration test results	X	
6. Develop recommendations for improved security methods	X	
7. Review and approve recommendations for improved security		X
8. Implement approved recommendations	X	

3.1.5.4 Security Incident & Audit Management Services

Security Incident and Audit Management Services are the activities associated with maintaining requirements in connection with Security Incident & Audit Management Services. The following table identifies the Security Incident and Audit Management roles and responsibilities that Vendor and VITA will perform.

Table 13. Security Incident & Audit Management Roles and Responsibilities

Security Incident & Audit Management Services Roles and Responsibilities	Vendor	VITA
1. Develop policies for Security Incident & Audit Management	X	
2. Approve policies for Security Incident & Audit Management		X
3. Provide initial review (Level 1) of security Incidents and the determination if escalation to Commonwealth IT Security (Level 2, 3 support) is warranted	X	
4. Identify and isolate from the Network any virus/worm infected System	X	
5. Identify and provide countermeasures for virus / worm attacks	X	
6. Provide escalation point for further review of security Incidents		X
7. Establish security audit policies		X

Security Incident & Audit Management Services Roles and Responsibilities	Vendor	VITA
8. Provide technical expertise for security audits	X	
9. Collect and review all incidents reported by all other security services (e.g., NIDS, HIDS, penetration testing, firewall)	X	
10. Maintain a central repository of log files in accordance with VITA and Commonwealth policies and Service Levels including application specific and System specific log files	X	
11. Provide security reporting	X	

3.2 Exclusions

The following items are specifically excluded from this SOW:

None identified

3.3 Service Specific Milestones

Milestones specific to the deployment of Security Services are listed in the following:

Milestone Description	Milestone Date
TBD – Vendor to provide as part of its Transition Plan	

4.0 Service Management

4.1 Objectives

A key objective of the Agreement is to attain Service Levels with Performance Credits where business is impacted through failure to meet significant mission critical Systems or Services, Critical Milestones or objectives, or when Service performance requirements are not met. Service Levels are detailed in the following sections and those associated with Performance Credits are identified in Schedule 3.12 (Service Level Methodology) of the Agreement..

Vendor shall provide written reports to VITA regarding Vendor's compliance with the Service Levels specified in this SOW.

4.2 Definitions

Appendix 10 (SOW Definitions) to Schedule 3.3 (Statements of Work) of the Agreement provides a list of terms that apply to this SOW and the following Service Levels.

4.3 Service Level Requirements

4.3.1 Security Services Service Levels

The following minimum Service Levels are required commencing on the Service Commencement Date. Vendor must consistently meet or exceed the following Service Levels. The Service Level methodology and the identification of Service Levels associated with Performance Credits are detailed in Schedule 3.12 (Service Level Methodology) of the Agreement. **All times referenced are in Eastern Time**.

NOTE: Vendor must provide recommended Minimum Performance % for each Service Level type identified in the Tables below.

Table 14. System Server Administration Service Levels

DEFINITION	Actions by Vendor for proactive monitoring and intervention to minimize capacity bottlenecks and activities required to implement system capacity and operational usage change requests.

System Server Administration Service Level Requirements			
System Server Administration Task	**Service Measure**	**Performance Target**	**Minimum Performance %**
System Security requests (RACF, ACF2)	Elapsed Time		
Deploy service / security patches / anti-virus updates necessary to fix/repair environment vulnerabilities	Elapsed Time		
	Formula	Number of requests completed within Performance Target /Total of all requests occurring during Measurement Interval	
	Measurement Interval	Measure Weekly, Report Monthly	
	Measurement Tool	TBD	

Table 15. Network Administration Services Service Levels

DEFINITION	Routers and circuits to be managed proactively using either product-specific or proprietary network monitoring and management tools and retain Network device logs for 45 days. Measurement for these Network components is 24x7x365 requirement. Pre-scheduled maintenance shall be preformed according to the published maintenance window schedule, with the ability to reschedule based on Network availability requirements from the various Eligible Customers.

Network Administration Services Service Level Requirements			
Network Administration Task	**Service Measure**	**Performance Target**	**Minimum Performance %**
Adding/deleting Vendor End-User accounts	Elapsed Time		

Network Administration Services Service Level Requirements			
Network Administration Task	**Service Measure**	**Performance Target**	**Minimum Performance %**
Firewall Management Implementation of firewall changes related to changing, adding/deleting firewall rules.	Elapsed Time		
	Formula	Transactions completed within Performance Target / Total Transactions	
	Measurement Interval	Monitor Continuously, Measure Daily, Report Monthly	
	Measurement Tool	TBD	

Table 16. Security Intrusion Detection / Prevention Service Levels

DEFINITION	Network traffic to/from designated systems is monitored for current attack signatures and logs retained for 45 days. Measurement for this Service is 7x24x365 requirement. Pre-scheduled maintenance shall be preformed on Sunday between the hours of 0100 to 0700.

Security Intrusion Detection Service Level Requirements			
Management Task	**Service Measure**	**Performance Target**	**Minimum Performance %**
NIDS / NIPS – monitor	Overall Schedule		
HIDS / HIPS – monitor for changes to selected local files	Overall Schedule		
NIDS / NIPS – review all positive Priority Level 1 and Priority Level 2 alerts and notify the Commonwealth by prescribed methods	Elapsed Time		
HIDS / HIPS – review all positive Priority Level 1 and Priority Level 2 alerts and notify the Commonwealth by prescribed methods	Elapsed Time		

Security Intrusion Detection Service Level Requirements			
Management Task	**Service Measure**	**Performance Target**	**Minimum Performance %**
NIDS / NIPS & HIDS / HIPS Implementation of changes related to changing, adding, and deleting signatures and rules	Elapsed Time		
	Formula	Performance = Transactions completed per Management Task within Performance Target / Total Transactions per Management Task occurring during the Measurement Interval	
	Measurement Interval	Monitor Continuously, Measure Daily, Report Monthly	
	Measurement Tool	TBD	

Table 17. Security Penetration Services Service Levels

DEFINITION	Entire Networks are tested to determine the susceptibility of their hosts to current attacks. Measurement for this Service is Mon-Fri, during Business Day Hours, for Intranet testing. Whereas Internet penetration testing occurs outside of Business Day Hours [1700 – 0700] and where appropriate, running continuously over the weekend. Pre-scheduled maintenance shall be preformed during periods of minimal service activity or as otherwise agreed upon by VITA.

Security Vulnerability & Penetration Services Service Level Requirements			
Management Task	**Service Measure**	**Performance Target**	**Minimum Performance Measure**
Testing of vulnerabilities	Overall Schedule		
	Formula	Transactions completed within required time / Total Transactions	
	Measurement Interval	Monitor Continuously, Measure Daily, Report Monthly	
	Measurement Tool	TBD	

Table 18. Account Administration Service Levels

DEFINITION	Routine functions, such as setting up End-User IDs, changing End-User authorization tables, changing account codes and similar functions, which are handled by Vendor.

Account Administration Service Level Requirements

Account Administration Service Level Requirements			
End-User Account Administration Tasks	**Service Measure**	**Performance Target**	**Minimum Performance %**
New End-User Account (up to 5 per request)	Elapsed time		
New End-User Account (6-20 per request)	Elapsed time		
New End-User Account (20+ per request)	Elapsed time		
Password Reset	Elapsed time		
Privilege Changes	Elapsed time		
Disable End-User Account	Elapsed time		
Terminate End-User Account	Elapsed time		
Procurement Request	Elapsed time		
	Formula	Number of instances within Performance Target / Total number of instances during Measurement Interval = "Percent (%) Attained"	
	Measurement Interval	First Month – Measure Daily, Report Weekly Thereafter – Measure Daily, Report Monthly	
	Measurement Method/Source Data	TBD	

4.4 Reports

Vendor shall provide written reports to VITA regarding Vendor's compliance with the Service Levels specified in Section 4.3. In addition, the following reports are required:

Table 19. Security Services Reports

Report Description	Timing
TBD– Example reports to be provided by Vendor as part of its response	

5.0 Referenced SOW Addenda

SOW Addenda	Description
Addendum 1	Hardware
Addendum 2	Software
Addendum 3	Commonwealth Facilities and IT Environments
Addendum 4	Removal of Commonwealth Data from Surplus Computer Hard Drives and

SOW Addenda	Description
	Electronic Media Standard - COV ITRM Standard SEC2003-02.1, dated March 8, 2004 - Revision 1